UNCLASSIFIED

National Telecommunications Security Working Group

NTSWG GUIDELINES FOR VOICE OVER INTERNET PROTOCOL (VoIP) COMPUTER TELEPHONY

NTSWG STANDARD 2(b)

April 2006

TABLE OF CONTENTS

PREFACE

This standard was prepared by the *National Telecommunications Security Working Group* (NTSWG). The NTSWG, formerly known as the *Telecommunications Security Group* (TSG), is a Joint Working Group of the *Committee on National Security Systems* (CNSS) which was established under EO 13231 to protect National Security Systems. The charter members of the NTSWG are: Department of the Air Force, Department of the Army, Central Intelligence Agency, Defense Intelligence Agency, Department of Energy, Federal Bureau of Investigation, Department of the Navy, National Reconnaissance Office, National Security Agency, US Secret Service, and the Department of State.

The NTSWG is the primary technical and policy resource in the US Intelligence Community for all aspects of the *Technical Surveillance Countermeasures* (TSCM) program involving telephone systems. The NTSWG standards contain guidance for providing on-hook security for telephone systems located in areas where sensitive government information is discussed. Implementation of NTSWG standards does not preclude the application of more stringent requirements and may not satisfy the requirements of other security programs such as TEMPEST, COMSEC, or OPSEC. This standard is a stand-alone standard that complements TSG Standard 2. TSG Standards 1, 2 and 6 (now administered by the NTSWG) are described below.

> <u>TSG Standard 1</u> (March 1990) is an introduction to telephone security that provides general information about the TSG standards.
>
> <u>TSG Standard 2</u> (released in March 1980) prescribes the fundamental requirements for planning, installing, maintaining, and managing *Computerized Telephone Systems* (CTSs). Although these requirements remain substantially unchanged, they need supplemental material to cover the many CTS advances that have occurred. These advances are primarily based on the increased integration of computer-automated tasks beyond those contained in early CTSs. For example, there have been changes in remote administration from *modem ports* to *Internet* and *Local Area Network* (LAN) connections. Additionally, the *Voice over Internet Protocol* (VoIP) computer telephony application, to which this standard applies, has been implemented. While these advances create new opportunities and benefits, they carry new security risks that require careful attention. TSG Standard 2 was developed to ensure that a CTS operated as an isolation point between the individual telephone instruments and the Dial Central Office. In a traditional CTS design, the only connection to an individual telephone was dedicated wiring between the telephone and the CTS. The telephone could only interface with the CTS. The CTS configuration was hardened to prevent telephone instruments from being configured with security-adverse features. The actual administration of the CTS was performed locally; otherwise security personnel approved short-term alternatives.
>
> <u>TSG Standard 6</u> (Updated January 2005) is a compilation of TSG-approved telephone security equipment. These items have been specifically evaluated by the NTSWG for security effectiveness.

In a VoIP configuration, the telephone instruments are connected via a distributed network to the “telephone switch.” The instrument’s connection, therefore, is no longer restricted to the "telephone switch" alone, but can be addressed by other devices on the network. Additionally, the VoIP telephone instrument is remarkably different from the conventional telephone attached to a traditional CTS. A VoIP instrument is essentially a *computer with a microphone and network connectivity* and many have a built-in web server to permit easier administration of its features. It follows that the administration of the "telephone switch" is no longer limited to a dedicated hardwire connection, but to a distributed network. This substantially reduces the security of the "telephone switch" that previously had sole control over the telephone configuration. Also, note that most traditional CTSs use *proprietary protocols* whereas most VoIP configurations use *open-standard protocols*. The use of an open-standard protocol increases the number of individuals who are knowledgeable about system commands, escalating the possibility that someone could *compromise* the system.[1]

Given these new VoIP-introduced concerns, simply applying TSG Standard 2 requirements to a VoIP application would not provide satisfactory telephone security. Although an earlier version of this VoIP Standard (NTSWG Standard 2(b)) was released in 2001 to cover the VoIP-introduced concerns, a new revision of that standard was needed to handle subsequent changes in VoIP technology and the associated risks that have emerged.

[1] Although VoIP introduces many new security concerns, it may reduce a few problems found in traditional telephones. For example, traditional analog telephone instruments can induce low-level signals onto the outgoing line. Occasionally, these signals transmit conversations occurring near the telephone. Some of these conversations may be recoverable by applying amplification equipment. In an IP environment, this is unlikely because low-level signals are not regenerated by the switches and routers. In effect, the switch or router acts as a disconnect since there is no "physical" connection through them.

PURPOSE

This document prescribes the standards for the secure implementation and use of a VoIP Telephony system in government (or government contractor) sensitive areas. The requirements established in this standard are necessary in order to achieve on-hook audio security for VoIP telephones and/or systems located in sensitive discussion areas.

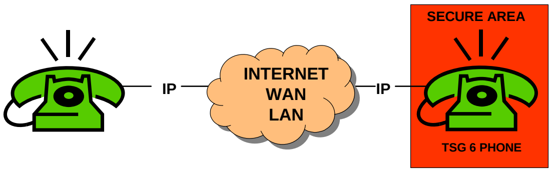
APPLICABILITY

This supplement applies to all unclassified *VoIP Telephony Systems* that are currently installed, or will be installed, in U.S. Government or U.S. Government sponsored contractor spaces where classified information is discussed (or when used as a point of isolation in accordance with TSG Standard 2).

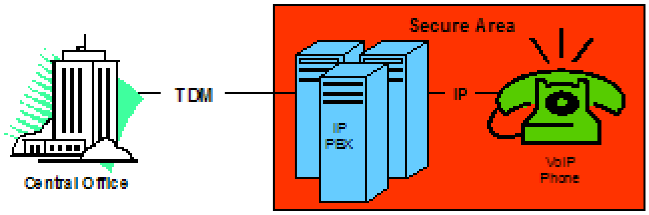
REQUIREMENTS

The requirements of this document cover the above VoIP Telephony Systems but do not specifically address network *Certification and Accreditation* (C&A) requirements that many Organizations mandate. Since VoIP networks may also need to conform to the specific C&A requirements of the individual Departments or Agencies, consult with your C&A authority for C&A guidance. The security requirements for each of the following configurations are specified in a separate annex which forms a part of this standard. General requirements are also discussed in the *Overview of VOIP Telephone System Security* section. (See Page 4.) It should be noted that as technology changes, the Annexes may be replaced to address those changes.

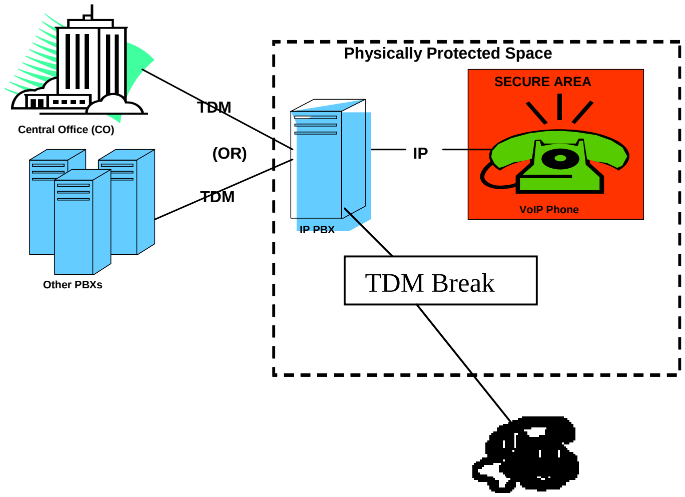
1. Pure VoIP *(See Annex A).* A *Pure VoIP* is IP-based for all end-to-end communications and signaling. Security in a Pure VoIP system is provided by TSG Standard 6 listed instruments.



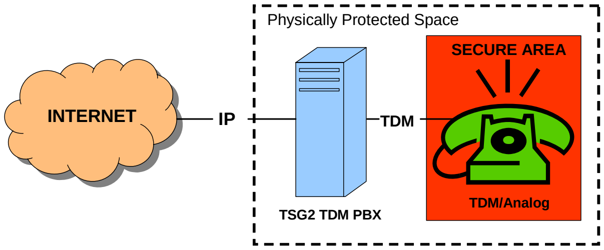
2, Isolated VoIP *(See Annex B).* An *Isolated VoIP* uses a mix of traditional *Time Division Multiplexing* (TDM) and VoIP technologies similar to *Hybrid VoIP*, but is exclusively for secure area use. The IP PBX, telephones, and associated wiring must be located in the secure area. Only the TDM trunk lines may be located outside the secure area.



3. Hybrid VoIP *(See Annex C).* A *Hybrid VoIP* uses a mix of traditional *Time Division Multiplexing* (TDM) and VoIP technologies to complete the end-to-end call. However, unlike *Isolated VoIP*, the IP PBX is not required to be located in the secure area. Rather, it must be located in a Physically Protected Space. All signal lines must be protected to the same level as the PPS.



4. VoIP Trunk (See Annex D). The trunk line is VoIP and the end telephonic device(s) and *Private Branch Exchange* (PBX) are TDM. Security is provided by either the Instrument or the TDM PBX.



OVERVIEW OF VOIP TELEPHONE SYSTEM SECURITY

Unclassified VoIP systems in secure areas shall not pass/transmit sensitive audio discussions when they are idle and not in use. Additionally, these systems shall be configured to prevent external control or activation. The concepts of "on-hook" and "off-hook" audio protection outlined in TSG Standards 2 and 6 must be incorporated into VoIP systems.

Unclassified VoIP telephone systems and services shall be configured to prevent technical exploitation or penetration. In addition, these systems shall incorporate physical and software access controls to prevent disclosure or manipulation of system programming and stored data. The following specific requirements are applied to unclassified VoIP systems:

- Provide on-hook audio protection by the use of TSG Standard 6 instrument(s) or equivalent TSG 2 system configuration.

- Provide off-hook audio protection by use of a hold feature, modified handset (push-to-talk), or equivalent.

- Provide isolation by use of a properly accredited VoIP computerized network with software and hardware configuration control and control of audit reports (such as station message detail reporting, call detail reporting, etc.). System programming will not include the ability to place, or keep, a handset off-hook. Configuration of the system must ensure that all on-hook and off-hook vulnerabilities are identified and mitigated.

- Equipment used for administration of VoIP telephone systems is installed inside an area where access is limited to authorized personnel. When local or remote administration terminals are not or cannot be contained within the controlled area, and safeguarded against unauthorized manipulation, then the use of TSG 6 approved telephone instruments shall be required, regardless of the VoIP Network configuration.

All unclassified VoIP systems and associated infrastructure must be electrically and physically isolated from any classified information/telecommunications systems in accordance with *National Security Telecommunications and Information Systems Security Committee* (NSTISSC) requirements.

Unclassified information systems must be safeguarded to prevent manipulation of features and software that could result in the loss/compromise of sensitive audio information or protected data. An unclassified VoIP network may be subject C&A.

DEFINITIONS

Following is a glossary of terms used in this standard and its annexes. In some cases, the term's definition may differ from that generally accepted in industry. In such a case, the term's definition supplied below is specifically intended for use in interpreting and implementing this standard and its annexes. Note that there are several definitions for a VoIP system/network. Some additional terms not appearing in this glossary are defined in TSG Standard 1 and TSG Standard 2.

Internet Protocol (IP). *Internet Protocol* (IP) is part of the TCP/IP family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages.

Internet Protocol Private Branch Exchange (IP PBX). An *Internet Protocol Private Branch Exchange (IP PBX)* is a private branch exchange that utilizes IP protocols in a packet switched environment. This includes all the computer and IP network resources required for the VoIP implementation.

Hybrid VoIP. A *Hybrid VoIP* is a VoIP configuration using a mix of traditional *Time Domain Multiplexing* (TDM) and VoIP technologies to complete an end-to-end call.

Isolated VoIP. An *Isolated VoIP* is a VoIP configuration that is exclusively for secure area use.

Other Network Protocols. Any other networking or management scheme in which data is transmitted or received. For example: Frame Relay, Asynchronous Transfer Mode.

Physically Protected Space (PPS). A *Physically Protected Space* (PPS) is a space within a physically protected perimeter. This area must be locked and access limited to cleared US personnel requiring access to the system.

Pure VoIP. A *Pure VoIP* is a VoIP configuration that is IP-based for all end-to-end communications and signaling.

Simple Network Management Protocol (SNMP). SNMP is a protocol enabling system administrators to monitor and manage a network of connected computers.

Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is the suite of communications protocols used on the Internet. While TCP and IP are the most commonly used, TCP/IP also includes several other protocols.

Voice Over Internet Protocol (VoIP). *Voice Over Internet Protocol* (VoIP) is a term used to describe the transmission of packetized voice using Internet Protocol and consists of both signaling and media protocols.

Voice over IP Firewalls. Voice over IP Firewalls primarily function at the Application Layer and protect against vulnerabilities specifically associated with VoIP as well as other telephony concerns. VoIP firewalls can dynamically open and close ports associated with call setup and teardown.

VoIP Trunk. A *VoIP Trunk* is a VoIP configuration in which the trunk line is VoIP and the end telephonic device(s) and *Private Branch Exchange* (PBX) are TDM.

Annex A

Pure VoIP
Security Requirements

This annex specifies security requirements for deploying a *Pure VoIP* voice/data solution. Since the user cannot control the *Pure VoIP* network, only telephone instruments listed in TSG Standard 6 may be used.

This document does not address the certification and accreditation (C&A) requirements that many Organizations require. Consult with your network accreditation authority for guidance.

A.1 The following provisions *must be* implemented to promote *on-hook* and *off-hook* [audio] security in VoIP telephone instruments. Telephone instruments are not to be removed from the secure area except for repair, maintenance, or disposal.

a. Microphone Disconnect. Microphones used to process audio for a VoIP (telephony) application must have a positive disconnect whereby the connection requires the user to manually enable and disable the microphone. This typically requires the removal of the speakerphone microphone.

b. Identifiable Telephones. Telephones must be easily identifiable as NTSWG approved.

c. Audio Reverse Flow. Speakers used to output audio from a VoIP (telephony) feature must be equipped with amplifier circuits (op-amps or one-way amplifiers) that prevent the reverse flow of audio from the speaker transmit talk path. Side tone circuits are permitted provided they merely feed transmit audio to the local speaker receive circuit.

d. Handset/Headset Disconnect. Handsets/headsets used to process audio for VoIP (telephony) applications must have a means to positively disconnect the microphone and earpiece element from the circuit when not in use. The disconnect must be hardware controlled and must not rely on software controls alone. Compliance may require the use of *Push-to-Talk* (PTT) handsets.

e. Hold/Mute Feature. The VoIP (telephony) application must feature a “hold” function whereby local audio is shunted from the circuit when active. Similarly, when the mute feature is enabled, audio is shunted from the circuit. The “hold” or “mute” feature must be enabled/disabled from the local end only and must not be reconfigurable from the distant/calling end of the circuit (i.e., such as a firmware feature). When the hold or mute features are enabled, the audio shunt must be designed to remove the audio path from the transmit circuit so that no digitized audio is present.[2] If these requirements cannot be met, *Push to Talk* (PTT) handsets are required.

[2] Some VoIP vendors have designed hold and mute features that “flip a bit” to indicate the activation of the feature, but permit the actual transport of audio along the network connection.

f. Telephone Audio Security. In accordance with NTSWG Standard 5 *On-hook Telephone Audio Security Performance Specifications*, telephones shall not be capable of transmitting nearby room audio (e.g., discussions) that could be processed and transmitted beyond the physically protected space while in the on-hook condition. NTSWG Standard 6 listed instruments are required in areas where classified information may be discussed.

g. Unnecessary Telephone Functionality. VoIP telephone instrument functionality shall be limited to typical telephony functions. Unnecessary functionality shall be disabled. Users of VoIP telephones shall not be able to view administrative settings or settings such as IP addresses or MAC addresses. (Note: Such information could enable a user to gain information about the network or potentially spoof a device and gain unauthorized access.)

h. Unnecessary Telephone Services. Services other than those necessary to process VoIP telephone conversations and related VoIP functions (e.g., call setup) shall be disabled. Web services or the ability to browse the web with a VoIP phone shall be disabled.

i. Speech Processing Software and Telephone Data Ports. Speech to text conversion capability shall not be enabled. To ensure data and voice segregation, the data port on the VoIP telephone device shall be disabled.

Annex B

Isolated VoIP
Security Requirements

This annex specifies security requirements for deploying an Isolated VoIP configuration where the VoIP system is located in a *secure area for which it provides exclusive service* and the only equipment or wiring outside the secure area are the TDM trunk lines. These requirements apply to a VoIP PBX that exclusively uses TDM trunk lines, whether copper or fiber. Any current or planned IP connectivity outside of the switch must follow the requirements listed in Annex A. No wireless capability is permitted. This document does not address the certification and accreditation (C&A) requirements that many Organizations require. Consult with your network accreditation authority for guidance. VoIP networks must be physically separated from other IP networks. NOTE: This install is similar to a traditional TSG Standard 2 installation in that the isolation is provided to the VoIP network by the TDM gateway. Specifically, when a telephone instrument is placed in the on-hook condition it will be disconnected at that point from the outgoing TDM trunks.

B.1 Voice Instrument Security. The following provisions *must be* implemented to promote on-hook and off-hook [audio] security in VoIP telephone instruments. Telephone instruments are not to be removed from the secure area except for repair, maintenance, or disposal.

a. **Microphone Disconnect.** Microphones used to process audio for a VoIP (telephony) application must have a positive disconnect whereby the connection requires the user to manually enable and disable the microphone. This typically requires the removal of any internal microphones

b. **Telephone Audio Security.** VoIP telephones shall not be capable of transmitting nearby room audio (e.g., discussions) that could be processed and transmitted beyond the physically protected space while in the on-hook condition.

c. **Telephone Functionality.** VoIP telephone instrument functionality shall be limited to telephony related functions.

d. **Speech Processing Software and Telephone Data Ports.** Speech processing software/ application shall not be enabled for any computerized applications. To ensure data and voice segregation, the data port on the VoIP telephone device shall be disabled.

e. **Firmware Upgrades and Configuration File Integrity.** A management process must be implemented to ensure that appropriate files are vendor signed and/or authenticated. The files must be tested to prevent downtime (or service disruption) caused by compatibility issues or undesired changes to the existing security profile.

B.2 Physical Security.

a. **Trunk Line Location.** Only the *Time Division Multiplexing* (TDM) trunk lines may transgress the secure area. The PBX shall be located as close to the demarcation point as practical. All system wiring interconnections will be organized to facilitate technical inspections

b. **Program Media Protection.** All program media such as tapes or disks must be provided physical protection to prevent unauthorized alterations.

c. **Program Master Copy.** An up-to-date master copy of the program must be maintained for confirmation and/or reloading of the operating program. This master copy must be verifiable as having been protected against unauthorized alteration. The current program master copy must be maintained in a physically protected storage container, separate from all other program media.

B.3 IP Private Branch Exchange (PBX) Security. Only the VoIP system administrators are permitted to make changes to the system configuration and programming. Users are restricted to the use of only VoIP instruments to change their personal preferences (ring tones, speed dial lists, etc).

a. Auditing. The auditing function must be configured to monitor successful and failed access attempts to the device, all configuration settings changes (or attempted changes), and any other management control functions. These audit logs shall be enabled by default and their contents reviewed regularly, in accordance with local security policies.

b. Access Control.

1) **Access Control Lists.** Access control lists shall be configured on the IP PBX to prevent administrative actions being performed from unauthorized devices. The system shall be configured such that administrative functions must be performed from an administrative workstation using a dedicated *out-of-band management network*. Secondary user authentication shall also be implemented (e.g., Authentication, Authorization, and Accounting Server).

2) **Privileged Account Protection.** If an *out-of-band management network* is not possible, an equivalent level of protection shall be provided for administrative usernames and passwords to prevent unauthorized disclosure of privileged accounts. These administrative usernames and passwords shall be protected in accordance with NIST 140-2 encryption via a secure protocol such as *Secure Shell* (SSH) or *Secure Socket Layer* (SSL).

3) **Usernames and Passwords.** Usernames and passwords (in accordance with security requirements) shall be required prior to providing access to the administrative functions of the IP PBX. In addition to required authentication, strong passwords shall be used. Such passwords must consist of a minimum combination of three of the four character types (i.e., Uppercase, Lowercase, Numbers, and Special Characters) and a minimum length of eight characters.

d. Patch Management. A patch management process must be implemented to ensure that the latest available security patches are applied. The patches must be tested to prevent downtime (or service disruption) caused by compatibility issues or undesired changes to the existing security profile.

Annex C

Hybrid VoIP
Security Requirements

This annex specifies security requirements for deploying a Hybrid VoIP voice/data solution. This solution is where the VoIP system uses a VoIP *Private Branch Exchange* (PBX) that is located outside of the secure area, but within a Physically Protected Space (PPS) that is also controlled by the organization having oversight of the secure area. The VoIP System may only use TDM trunk lines, whether copper or fiber, for connectivity to other phone systems external to the PPS or central office. No wireless capability is permitted. (**Note:** This Annex covers hybrid VoIP configurations wherein the VoIP system also provides phone support to areas *outside* the secure areas. Hybrid VoIPs exclusively for secure area use are defined as *Isolated VoIPs* and are covered in Annex B of this standard.)

This document does not address the certification and accreditation (C&A) requirements that many organizations require. Consult with your network accreditation authority for guidance. VoIP networks must be either physically separated or have logical VLAN separation from other IP networks to ensure isolation between voice and data networks. Physical separation of the networks provides a higher level of security and is the preferred method of isolation. Any IP connectivity from the voice network to other LANs, WANs or Internet negates this solution and requires compliance with Annex A. IP trunking is not allowed in this configuration.

Under this solution, the VoIP server may also provide telephone support to areas *outside* the secure area. In this instance, the VoIP telephones used outside the secure area must meet the security requirements listed in paragraphs C.2.c.2), Wiring Isolation. Additionally, these phones require a TDM break located within the PPS. Other methods that provide a similar level of isolation may be approved by the NTSWG.

C.1 Voice Instrument Security. The following provisions *must be* implemented to promote on-hook and off-hook [audio] security in VoIP telephone instruments. Telephone instruments are not to be removed from the secure area except for repair, maintenance, or disposal.

a. **Microphone Disconnect.** Microphones used to process audio for a VoIP (telephony) application must have a positive disconnect whereby the connection requires the user to manually enable and disable the microphone. This typically requires the removal of any internal microphones.

b. **Identifiable Telephones.** Telephones must be easily identifiable as meeting the security requirements of this Annex.

c. **Handset/Headset Disconnect.** Handsets/headsets used to process audio for VoIP (telephony) applications must have a means to positively disconnect the microphone and earpiece element from the circuit when not in use. The disconnect must be hardware controlled and must not rely solely on software controls. Compliance may require the use of *Push-to-Talk* (PTT) handsets.

d. **Hold/Mute Feature.** The VoIP (telephony) application must feature a “hold” function whereby local audio is shunted from the circuit when active. Similarly when the mute feature is enabled, audio is shunted from the circuit. The “hold” or “mute” feature must be enabled/disabled from the local end only and must not be reconfigurable from the distant/calling end of the circuit (i.e., such as a firmware feature). When the hold or mute features are enabled, the audio shunt must remove the audio path from the transmit circuit so that no digitized audio is present.[3] If these requirements cannot be met, *Push to Talk* (PTT) handsets are required.

e. **Telephone Audio Security.** VoIP telephones shall not be capable of transmitting nearby room audio (e.g., discussions) that could be processed and transmitted beyond the physically protected space while in the on-hook condition.

f. **Unnecessary Telephone Functionality.** VoIP telephone instrument functionality shall be limited to typical telephony functions. Unnecessary functionality shall be disabled and administratively protected by use of a password or other approved method. Users of VoIP telephones shall not be able to view administrative settings or settings such as IP addresses or MAC addresses. (Note: Such information could enable a user to gain information about the network or potentially spoof a device and gain unauthorized access.)

g. **Unnecessary Telephone Services.** Services other than those necessary to process VoIP telephone conversations and related VoIP functions (e.g., streaming audio, call setup, call breakdown) shall be disabled if not needed. Web services or the ability to browse the web with a VoIP phone shall be disabled.

h. **Speech Processing Software and Telephone Data Ports.** Speech processing software/ application shall not be enabled for any computerized applications. To ensure data and voice segregation, the data port on the VoIP telephone device shall be disabled.

i. **Firmware Upgrades and Configuration File Integrity.** A management process must be implemented to ensure that any installation or upgrade of program or data files originate from the vendor. These upgrades must be tested to prevent downtime (or service disruption) that may be caused by compatibility issues or undesired changes to the existing security profile. Data network security is required to ensure that upgrades do not originate from unintended sources outside of the secure area.

C.2 Voice/Data Network.

a. **Server Security.** The hardening of critical network components (e.g., call processor/ controllers, media/signaling gateways) is crucial to a VoIP system’s security because of the functionality they provide. Server systems have a relatively large level of exposure due to the functions and services that they typically provide. There are additional security concerns associated with VoIP functionality as vulnerabilities that are inherent in the server operating

[3] Some VoIP vendors have designed hold and mute features that “flip a bit” to indicate the activation of the feature, but permit the actual transport of audio along the network connection.

systems are more readily exposed and will be introduced into the telephony system and must be addressed.

1) **Operating System Hardening.** Operating systems hardening shall be performed in a manner consistent with approved hardening guidelines such as *National Security Agency* (NSA) Security Configuration Guides or *Defense Information Systems Agency* (DISA) Security Technical Implementation Guides. DISA has developed several guides that address operating system, network, and device hardening techniques. This level of hardening shall be performed on all management workstations or devices with similar functionality.

2) **Patch Management.** A patch management process must be implemented to ensure that the latest available security patches are applied. The patches must be tested to prevent downtime (or service disruption) caused by compatibility issues or undesired changes to the existing security profile.

3) Ethernet Port Security shall be configured on switch devices to reduce the risk of an attacker collecting data (using a network-based H.323/SIP data sniffer) and replacing a legitimate telephony device with a rogue device such as a laptop or palmtop.

b. **Network Perimeter Security.** Perimeter Security, whether VoIP or otherwise, plays a key role in the overall security of the network. A combination of both a traditional firewall and a VoIP Application-Layer Firewall shall be applied to perimeters of the secure area and between VLANs.

c. Physical Security.

1) **Physically Protected Space (PPS).** A *physically protected space* (PPS) must be established to provide positive physical protection for the VoIP system and all of its components and interfaces. This includes all telephones, cables, lines, intermediate patch panels, servers, routers and switches necessary for the functioning of the system. The PPS must be controlled by the organization having oversight of the secure area.

2) **Wiring Isolation.** Only equipment or wiring *not* intended to be isolated by the VoIP system may be located outside of the PPS. However, to ensure data and voice segregation, the data port on all VoIP telephone devices shall be disabled. Additionally, users of all VoIP telephones shall not be able to view administrative settings or settings such as IP addresses or MAC addresses.

3) **Program Media Protection.** All program media such as tapes or disks must be provided physical protection to prevent unauthorized alterations.

4) **Program Master Copy.** An up-to-date master copy of the program must be maintained for confirmation and/or reloading of the operating program. This master copy must be verifiable as having been protected against unauthorized alteration. The

current program master copy must be maintained in a physically protected storage container, separate from all other program media.

C.3 IP Private Branch Exchange (PBX) Security. The use of IP, Ethernet, or other *local area network* (LAN) connections can provide new methods for performing administration and maintenance of *IP Enabled Private Branch Exchanges* (IP PBX's). While such use may result in lower administrative overhead costs, such use may also introduce vulnerabilities not found in traditional telephony implementations. With such use, the IP PBX is potentially susceptible to IP-based network attacks that could permit unauthorized access. To prevent unauthorized access to the IP Enabled PBX's programming, settings, and configurations, the following requirements must be met.

a. **Auditing.** The auditing function must be configured to monitor successful and failed access attempts to the device, all configuration settings changes (or attempted changes), and any other management control functions. These audit logs shall be enabled by default and their contents reviewed regularly, in accordance with local security policies.

b. Access Control.

1) **Access Control Lists.** Access control lists shall be configured on the IP PBX to prevent administrative actions being performed from unauthorized devices. The system shall be configured such that administrative functions must be performed from an administrative workstation using a dedicated out-of-band management network. User authentication shall also be implemented (e.g., Authentication, Authorization, and Accounting Server). These connections must be protected with NIST 140-2 approved encryption protocols.

2) **Privileged Account Protection.** If an out-of-band management network is not possible, an equivalent level of protection shall be provided for administrative usernames and passwords to prevent unauthorized disclosure of privileged accounts. These administrative usernames and passwords shall be protected in accordance with NIST 140-2 encryption via a secure protocol such as *Secure Shell* (SSH) or *Secure Socket Layer* (SSL).

3) **Usernames and Passwords.** Usernames and passwords (in accordance with security requirements) shall be required prior to providing access to the administrative functions of the IP PBX. In addition to required authentication, strong passwords shall be used. Such passwords must consist of a minimum combination of three of the four character types (i.e., Uppercase, Lowercase, Numbers, and Special Characters) and a minimum length of eight characters.

Annex D

VoIP Trunk
Security Requirements

This annex specifies security requirements for deploying a VoIP Trunk voice/data solution. This annex does not provide specific implementations needed to satisfy each requirement. This type of VoIP implementation consists of a traditional *Time Division Multiplexing* (TDM), *Computerized Telephone Systems* (CTS) using VoIP for an external trunk. These requirements apply if the VoIP Trunk cards of the PBX convert IP to Time Division Multiplexing. If the trunk cards provide any other support for IP, the system must meet the requirements of the applicable Annex in this document. The requirements of this document do not address the certification and accreditation (C&A) requirements that many Organizations require. Consult with your network accreditation authority for guidance.

D.1 **Voice Instrument Security.** Voice instrument security may be accomplished by using one of the following two methods.

Method #1: Use TSG Standard 6 approved phones or interface devices.
Method #2: Use TSG Standard 2 guidelines for securing telephone systems (see C.2)

D.2 **Private Branch Exchange (PBX) Security.** The PBX must comply with the installation and maintenance requirements detailed in TSG Standard 2.